TNI Module Three

Network Component Evaluation and Composition

This module is the third of four modules that describe the use of the Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC) for network product evaluation and certification. The basic terms and concepts presented in the TNI are summarized in TNI Module One. TNI Module Two presents Part I of the TNI, which provides TCSEC interpretations for complete network systems. This module describes the rationale for NTCB partitions and interpretations of the TCSEC for network component evaluations presented in Appendices A and B of the TNI. A network system or component may also offer other security services (e.g., non-repudiation, denial of service). These security services and guidelines for their ratings are presented in TNI Module Four.

Module Learning Objectives

TNI Module Two introduced the concept of a partitioned NTCB. This module builds on the partitioned network concept with the evaluation and composition of network components. Upon completion of this module the student should understand:

1) the rationale for network decomposition.

2) the types of network components, their evaluation requirements, and class ratings.

3) how to compose network components, the applicable rules, and class ratings.

Overview

The TNI allows for the evaluation of both network systems and network components. A network system enforces a complete network security policy and encompasses an entire NTCB. To be complete, all network devices along with their software must be known at the time of evaluation and included in the evaluated configuration.

A network component enforces a portion of an overall network security policy and encompasses only a portion of the NTCB, a NTCB partition. For example, a network component may only provide mechanisms that implement a mandatory access control (MAC) policy. These components can be composed with other network components to form a complete NTCB and support an overall network security policy.

Network systems, evaluated under TNI Part I and discussed in TNI Module Two, are considered complete and not intended to be composed with other network components. They are not evaluated with the idea of composition in mind. As a result, a network system evaluation cannot be reused in the event that the evaluated network system is composed with another network system or component. Network components, however, are designed and evaluated

with the intention that they will be composed with other network components. A network component evaluation may be reused for every subsequent composition with a network system or component. The evaluation of the resulting component or system is greatly simplified by preserving the rating of the original evaluated network component, in accordance with TNI network composition rules.

Rationale for NTCB Partitions

The network component evaluation requirements presented in TNI Appendix A are intended to support an eventual network system evaluation or certification using TNI Part I. A major issue concerning the use of the partitioned NTCB view is how to partition the network into network components for evaluation. TNI Appendix B provides a theoretical example for partitioning a network. The example describes an application running on a stand-alone system simulating a network of NTCB partitions. The simulation then undergoes a series of transformations that convert it into a single NTCB partitioned network. The conversion of a partitioned NTCB into a single NTCB demonstrates the inverse, that partitioning of a single NTCB, is conceptually sound. Read TNI Appendix B, for more technical and theoretical detail.

Network Components

The TNI identifies four types of security policies that may be provided by a network component: 1) Mandatory Access Control, 2) Discretionary Access Control, 3) Identification and Authentication, and 4) Audit. They are identified by one-letter designations M, D, I, and A, respectively. A network component can provide any combination of M, D, I or A functionality, so that there are fifteen different network component types which can be evaluated. In addition to the type designator based on the policy or policies supported, an evaluated network component is assigned a single evaluation class for which it meets all applicable requirements (according to TNI Appendix A).

Component Requirements

Generally network components may be evaluated against the TNI Part I requirements without further interpretation. However, the variance between complete network systems and network components motivate some difference in the interpreted requirements. A listing of the differences in the interpreted requirements may be found in TNI Appendix A. A description of some of the general rules applied in Appendix A modifications to the Part I interpretations follows:

The partitioning of the NTCB among the policy boundaries (M, D, I, and A) leads to a natural division of the TCSEC requirements along the same boundaries. All network components, regardless of the policy enforced, must adhere to the TCSEC object reuse, documentation and assurance requirements at the class of the evaluation. Network components enforcing DAC, I&A, and/or audit policies are required to meet the associated DAC, I&A, and/or Audit requirements. Network components that enforce a MAC policy are required to meet the policy label requirements (e.g., label integrity, labeling human-readable output)[1] and the high assurance requirements (e.g., design

specification and verification, trusted recovery) in addition to meeting the MAC requirements. Only network components that enforce a MAC policy require the use of labels or offer high assurance.

Network components, regardless of the policy supported, must produce audit data for any action performed on the component which may lead to a violation of an overall network policy. Network components that do not support an audit policy must provide a mechanism for making the audit data they produce available to an audit component. For example, an I-Component must produce audit data concerning multiple logon attempts. The I-Component does not support an audit policy and must relay the audit data to a network component which uses this data to support an audit policy.

Component Ratings

Each network component type has a minimum and maximum class that may be achieved. The minimum class is that TCSEC class which first imposes a requirement relevant to that network component type. The maximum class is the class which imposes the highest requirement relevant to the network component type. Changes in their associated requirements, and the resulting rating range of the four network component policies are presented in Table 3-1.

Component Type	Additional Requirements at Class						Rating Range
	C1	C2	B1	B2	B3	A1	
M			X	X	X	X	B1 - A1
D	X	X			X		C1 - C2+
I	X	X	X				C1 - C2
A		X	X	X	X		C2 - C2+

Table 3-1: Network component rating ranges

The range of evaluation class ratings possible for a M-Component is a straightforward mapping of the classes in which a MAC requirement has been added or changed. The rating ranges for the D, I, and A-Components, however, do not directly reflect the changes in their requirements between the evaluation classes. This is described in the following paragraphs.

A D-Component can be evaluated to meet the C1 or C2 class. The TCSEC DAC requirements at C1 and C2 provide the basis for the C1 and C2 D-Component requirements. At B3 the TCSEC requires the use of ACLs for each named object. A D-Component, which provides this type of service, may be evaluated at the C2+ class. The B3 notation is not used in this instance, since the C2+ D-

[1] In the TNI, the requirements for Exportation of Labeled Information and Exportation to Single-Level Devices are absent from the requirements for a M-component. This oversight has since been formally acknowledged (on the TNI_Discussion forum of Dockmaster). The student should assume the inclusion of both of these requirements for M-components.

Component is not required to meet the B3 assurance requirements (e.g., Design Specification and Verification, Configuration Management)[2].

An I-Component can be evaluated to meet the C1 or C2 class. The TCSEC I&A requirements at C1 and C2 provide the basis for the C1 and C2 I-Component requirements. At B1 the TCSEC requires that the authentication data maintained by the TCB include clearances and authorizations (to be used for MAC enforcement). An I-Component rating above C2 is not available for an I-Component which provides this service[3].

An A-Component can be evaluated to meet the C2 class. The C2 TCSEC Audit requirements provide the basis for the C2 TNI A-Component requirements. At B1 the TCSEC requires additional audit capabilities based on sensitivity levels. The B2 TCSEC Audit requirements include the ability to audit covert channels. At B3 the TCSEC requires administrator notification when thresholds of selected audit events are exceeded, signaling imminent danger of security policy violations. An I-Component being evaluated at the C2+ class must meet the B3 TCSEC Audit requirements, which comprise all Audit requirements mentioned above. The B3 digraph is not used in this instance, since the C2+ A-Component is not required to meet the B3 assurance requirements (e.g., Design Specification and Verification, Configuration Management). Note that although the TCSEC refined the requirements for audit over four evaluation classes (C2 - B3), the TNI only offers two classes for A-Component ratings: C2 and C2+. The implications of the reduced number of evaluation classes for audit components is discussed in the composition ratings section of this module.

TNI Appendix A presents a table containing the rating range for all fifteen network component types. Table 3-1 and the explanation above only presents the rating ranges for single policy network components. The class range for network components that support multiple policies result from an application of the ranges of the single policy network components. In order to provide the student with a greater understanding of the rationale for these rating ranges, the following rule is presented for network components that support multiple policies:

Rating Range Rule: Network components enforcing multiple policies have both a minimum and maximum achievable rating. The minimum rating is equal to the highest minimum rating among the network components supporting the

---

[2] The belief that DAC, I&A, and Audit policies do not benefit from high assurance is also reflected in the network system evaluations (TNI Module Two). The TNI states (4.1.3.2.2), "The FTLS must represent the underlying reference monitor and any subjects implementing the mandatory policy. Other policy elements distributed in NTCB subjects ...need not be represented by the FTLS."

[3] Since clearances and authorizations are used in conjunction with a MAC policy, the composition of any I-component with a M-component must ensure the provision of this type of service.

single policies. The maximum rating is equal to the highest maximum rating among the network components supporting one of the single policies.

For example, the range of classes in which a DIA-Component may be evaluated is computed using the Rating Range Rule and Table 3-2. A DIA-Component will have a rating range of the highest minimum and maximum rating of the policies it supports: D, I, and A. The highest minimum rating of D, I, and A is the minimum rating of an A-Component: C2. The highest maximum ratings of D, I, and A is the maximum ratings of both the D and A-Components: C2+. Therefore, the rating range of a DIA network component is C2 - C2+.

Policy Supported	Minimum Rating	Maximum Rating
M	B1	A1
D	C1	C2+
I	C1	C2
A	C2	C2+

Table 3-2: Single policy minimum and maximum ratings

Network Component Compositions

An evaluated network component may be combined with other network components to form a network system or another network component. In the case that the resulting configuration forms a complete network system, Part I of the TNI is used for the evaluation or certification. If a new network component is formed and at least one of the combined network components has not been evaluated, the resulting network component is evaluated as a network component. In the case that the combined network components have all previously been evaluated, a network composition results, which does not need to be re-evaluated.

Composition Requirements

In order for a network system composed of evaluated network components to be given a rating, the network components must be connected so that the policy and assumptions for each network component are not violated. The composition rules in Appendix A of the TNI are presented as a listing of requirements for every possible combination of evaluated network components. The rules are introduced in this module as a means of allowing the student to understand the rationale behind the composition requirements.

Policy Preservation Rule: Whenever network components are composed the resulting network component must preserve the original network components' policy. A protocol for communicating policy information between connected network components as well as a protocol definition may be necessary.

In the case that two or more M-components are connected, the composition rules of the TNI ensure that the MAC policy will be supported. The M-components can be connected via a single or multilevel channel. M-components connected by a single level connection must have the same sensitivity level. M-components connected through a multilevel channel, however, must support a labeling protocol to guarantee the meaning of the labels is interpreted correctly across the NTCB partitions.

If a network DAC policy is defined such that access decisions are based on user membership in network groups (i.e., user of host), the passing of identifiers is not needed. DAC components which base access decisions on individual user identification and hence require identification data to be passed between connected network components must provide and support an identification data passing protocol.

Identification-Authentication and Audit are considered supporting policies, (i.e., they support mandatory and discretionary access control policies: MAC and DAC). Identification and Authentication provides a means of identifying users and their clearances for access control purposes. Audit provides accounting information of all actions which may be construed as an attempt to violate an access control policy.

Components which are composed of an access control policy and a supporting policy (e.g., MDA-Component), need not support or provide a protocol for exchanging the supporting policy's information. If this protocol is not supplied, the resulting component may be composed only with other components that are also self sufficient with respect to the supporting policy (e.g., MA). The inclusion of such a protocol allows for a component to provide supporting policies to other components.

When composed components contain supporting policies yet lack an access control policy (i.e., I, A, IA), a protocol for exchanging the supporting policy's information is required. Since components of this type offer services which support the MAC and DAC policies, this protocol will be used for the inevitable connection to a component with an access control policy.

Network System Equivalence Rule: Whenever the resulting network component supports directly connected users, the network component must minimally meet the network system requirements (TNI Part I) at minimum class in which these policies are present.

Class	Policies Present
C1	DAC, I&A
C2	DAC, I&A, Audit
B1	MAC, DAC, I&A, Audit

Table 3-3: Minimum Class of Policy Inclusion

Using Table 3-3, a DA-component, which has a minimum rating of C2, is lacking the I&A policy which is present at C1 and above classes. The DIA-component, however, enforces all policies present in a C2 network system. A DIA-Component which supports directly connected users must meet all the network system requirements for class C2. A DA-Component which also supports directly connected users need not meet all the C2 network system requirements.

Composition Ratings

Network components composed of previously evaluated components receive a rating based on the ratings of the evaluated components and the policies enforced by the combined network component.

Composed Component Rating Rule: The composed network component rating shall be equal to the highest class for which it meets all network system requirements for each policy enforced by the composed component.

Table 3-4 shows the minimum rating required of each evaluated component policy for the composed components' desired class. For example, evaluated network components included in a B2 composed component must have a minimum evaluation class rating of B2, C2, C2, and C2 for MAC, DAC, I&A, and Audit policies respectively. These minimum ratings are indicated in column B2 of Table 3-4.

Component Policies	Composed Component Rating					
	C1	C2	B1	B2	B3	A1
MAC			B1	B2	B3	A1
DAC	C1	C2	C2	C2	**C2+**	**C2+**
I&A	C1	C2	C2	C2	C2	C2
Audit		C2	C2	C2	**C2+**	**C2+**

Table 3-4: Minimum component policy ratings required for composed component rating

In the case that the composed component comprises more than one given policy from its' components, each policy must meet the minimum rating. For example, the composition of a B1 MI-component with a B2 MA-component results in a B1 MIA-component, since the part of the MAC policy in the resulting component meets only B1 requirements.

The simplicity of the Composed Component Rating Rule is obscured by the introduction of the C2+ class for both DAC and Audit policies. Network system DAC requirements only change at C1, C2 and B3. The rating available to an evaluated D-Component are C1, C2 and C2+. To achieve the C2+ rating the D-Component must associate ACL's with all objects (a B3 requirement). A composed MD-Component wishing to receive a rating of B3 or above must

provide C2+ DAC. However, a composed MD-Component is not required to meet C2+ DAC in order to achieve a B1 or B2 rating.

Although network system Audit requirements change at C2, B1, B2, and B3, the ratings available to an evaluated A-Component are only C2 and C2+. The B1 - B3 network system Audit requirements are collapsed into a single class: C2+. To achieve the C2+ rating the A-Component must meet B3 network system Audit requirements. A composed MA-Component is not required to meet C2+ Audit in order to achieve a B1 or B2 rating[4]. However, a composed MA-Component wishing to receive a rating of B3 or above must provide C2+ Audit.

Required Readings

The required readings are supplied as part of the source material for the module. These readings, and the module overview, provide all the material covered by the module test questions.

DTNI87National Computer Security Center, *Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria*, NCSC-TG-005, 31 July 1987.

Other Related Readings

JKIN90 Greg King, *"Considerations for VSLAN Integrators and DAAs"*, Proceedings of the 13th National Computer Security Conference, pp. 201-210, 1990.

DEPL90 National Computer Security Center, *Final Evaluation Report, Verdix Corporation, VSLAN 5.0*, CSC-EPL-90/001, 25 July 1990.

DEPL91 National Computer Security Center, *Final Evaluation Report, Boeing Space and Defense Group, MLSLAN Secure Network Server System*, CSC-EPL-91/005, 28 August 1991.

DTNI87 National Computer Security Center, *Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria*, NCSC-TG-005, 31 July 1987.

---

4. The B1, B2, and B3 TCSEC Audit requirements have been folded into the C2+ class. The result of this collapsing of requirements is that a C2 A-component, which does not meet B1 or B2 TCSEC Audit requirements, may be composed with an M-component and receive a B1 or B2 MA-composition rating (depending on the class of the M-component). Clearly, a B1 MA-component should have audit records that include objects sensitivity labels and have the ability to audit the override of human-readable output (B1 TCSEC Audit requirements). In the same light, a B2 MA-component should be able to audit identified covert channel events (B2 audit requirement). Although, these requirements are not explicitly required for B1 and B2 MA-components.

JADD88 K.P. Addison, J.J. Sancho, *"Secure Networking at Sun Microsystems, Inc."*, Proceedings of the 11th National Computer Security Conference, pp. 212-218, 1990.

JTHO90 M. Thompson, R. Schell, A. Tao, T. Levin, *"Introduction to the Gemini Trusted Network Processor"*, Proceedings of the 13th National Computer Security Conference, pp. 211-217, 1990.

JKIN89 Greg King, *"A Survey of Commercially Available Secure LAN Products"*, Proceedings of the 5th Annual Computer Security Applications Conference, pp. 239-247.

JMAL90 P. W. Mallett, *"An Example Application of the Trusted Network Interpretation"*, Proceedings of the Sixth Annual Computer Security Applications Conference, pp. 9-19, December, 1990.